FAA National Software Conference, June 2001
DO-248B Overview

DO-248B Overview

Leanna Rierson
June 5, 2001

1

Presentation Outline

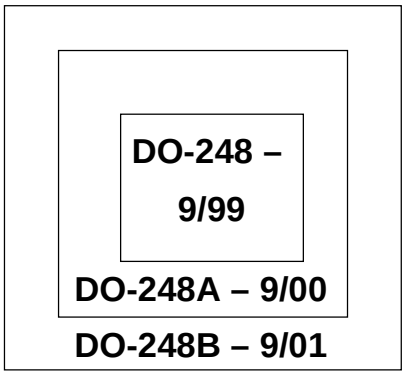
- History of DO-248[ ]
- DO-248B Layout
- FAA's Perspective on DO-248B
- Ways to Use DO-248B
- Major Topics of DO-248B
- Other Interesting Topics
- Summary

2

FAA National Software Conference, June 2001
DO-248B Overview

History of DO-248B

- Written by SC-190/WG-52 to Clarify DO-178B



3

History of DO-248B (cont)

- Created by 3 Teams
  - Development Team
  - Verification Team
  - Special Considerations Team
- Committee Consensus
- Edited by Editorial Team
- Published by RTCA & EUROCAE
- EUROCAE Equivalent is ED-94[ ]

4

DO-248B Layout

- **Introduction**
- **Errata (12)**
- **Frequently Asked Questions (FAQs) (76)**
- **Discussion Papers (DPs) (15)**
- **Appendices A-F**

5

FAA's Perspective

- DO-248[ ] is a clarification document
- It is not considered a guidance document

6

Ways to Use DO-248B

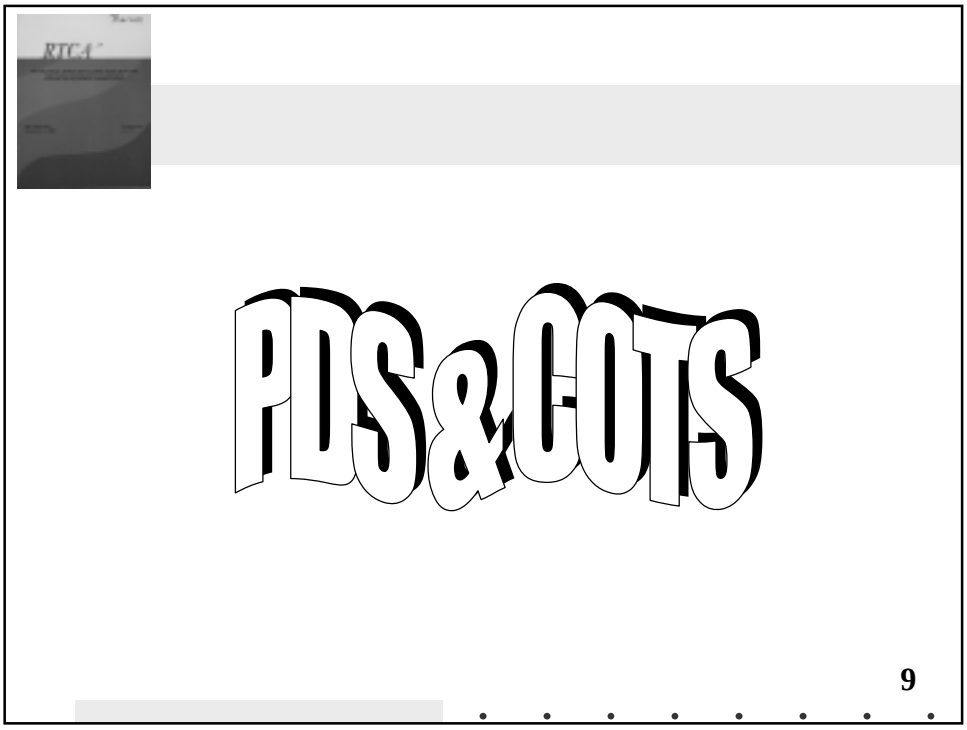
- Use it as a Sleep Aid (not recommended)
- Read it Straight Through (not recommended)
- Use Keyword Searches (Appendix C)
- Use Correlation to DO-178B (Appendix D)

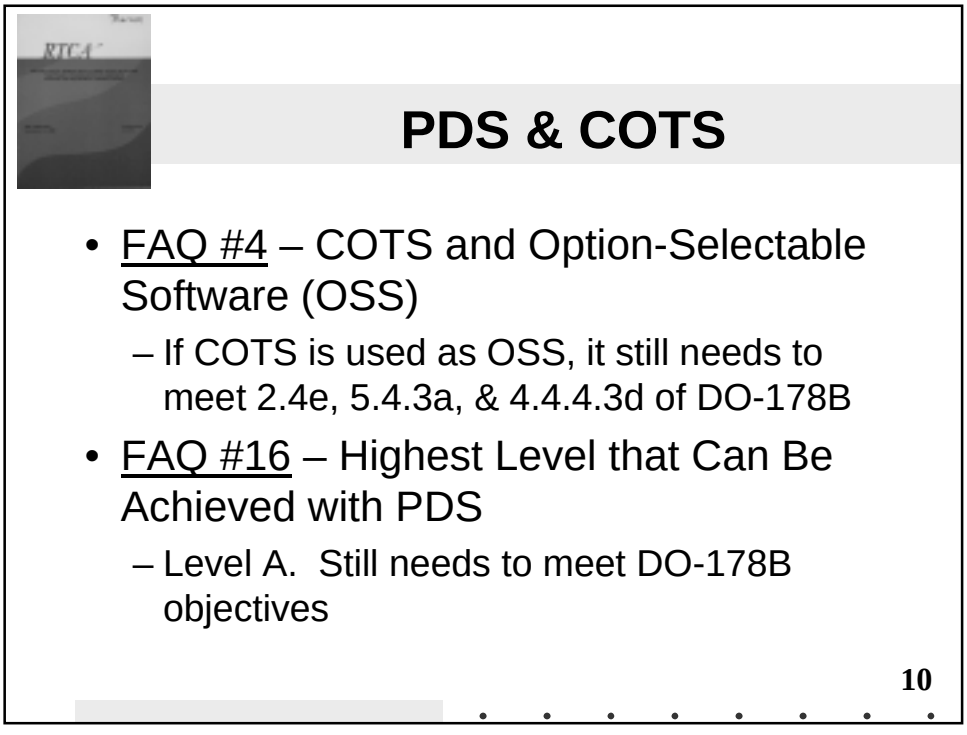
7

Major DO-248B Topics

- Previously Developed Software (PDS) and COTS Software
- Verification
- Service History
- Tools
- Control Categories

8


PDS&COTS
9


PDS & COTS
• FAQ #4 – COTS and Option-Selectable Software (OSS)
– If COTS is used as OSS, it still needs to meet 2.4e, 5.4.3a, & 4.4.4.3d of DO-178B
• FAQ #16 – Highest Level that Can Be Achieved with PDS
– Level A. Still needs to meet DO-178B objectives
10

PDS & COTS (cont)

- FAQ #17 – Changes to PDS
  - Need to Consider Impact On:
    - Requirements
    - Safety assessment
    - Data package/Documentation
    - Re-verification

11

PDS & COTS (cont)

- FAQ #25 – Using Architectural Means to Reduce PDS Software Level
  - Might consider things like:
    - Partitioning
    - Safety Monitoring
    - Restricted Functionality
  - Also consider:
    - Dead/Deactivated Code
    - Primary/Secondary functionality
    - Common Cause failures/errors

12

PDS & COTS (cont)

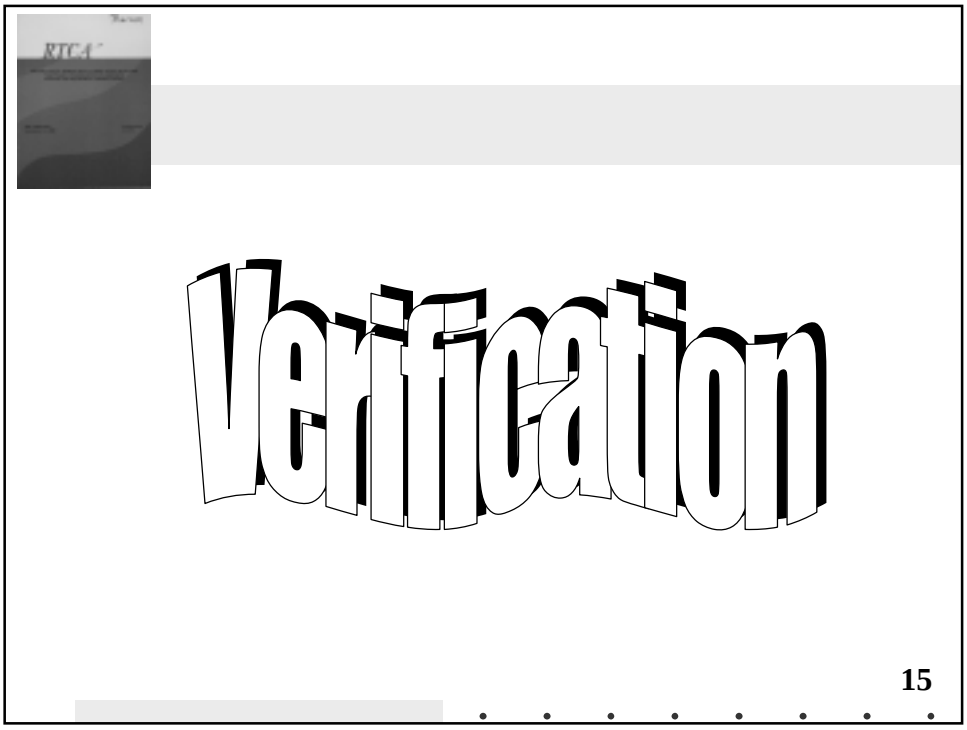
- DP #5 – Alternate Methods for PDS Compliance
  - 7 Alternate Methods are Discussed
    - Process Recognition
    - Prior Product Certification
    - Reverse Engineering
    - Restriction of Functionality
    - Product Service History
    - Formal Methods
    - Audits & Inspections

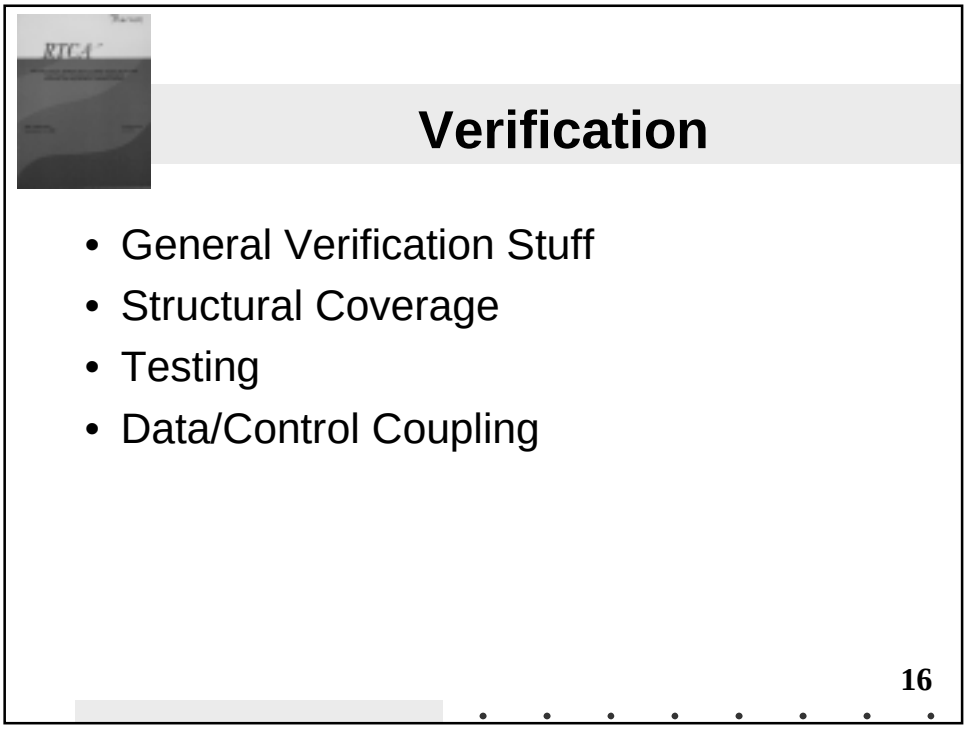
13

PDS & COTS (cont)

- DP #10 – Considerations for Using COTS
  - Technical Considerations
    - System safety context, supplier cert experience, availability of data, etc.
  - Business Considerations
    - Cost Considerations
    - Schedule Considerations

14


Verification
15


Verification
• General Verification Stuff
• Structural Coverage
• Testing
• Data/Control Coupling
16

Verification - General

- FAQ #26 – Independence in multi-version dissimilar software
- FAQ #31 – Verification relationships to the compiler acceptability
- FAQ #56 – Redundancies of verification documentation
- FAQ #58 – Implementing re-verification
- FAQ #63 – Exhaustive input testing

17

Verification – General (cont)

- FAQ #75 – Sampling in the verification process
- DP #1 – Verification tool selection considerations
- DP #7 – Definition of verification terms

18

Verification – Structural Coverage

- FAQ #42 – Performing structural coverage on the object code
- FAQ #43 – Intent of structural coverage analysis
- FAQ #44 – Structural testing vs. structural coverage analysis
- FAQ #74 – Difference between Level A and Level B
  - MC/DC and Independence

19

Verification – Structural Coverage (cont)

- DP #3 – Differences of DO-178A and DO-178B regarding structural coverage
- DP #8 – Tie between structural coverage and safety objectives
- DP #12 – Object code to source code traceability
- DP #13 – Definitions of statement coverage, decision coverage, & MC/DC

20

Verification - Testing

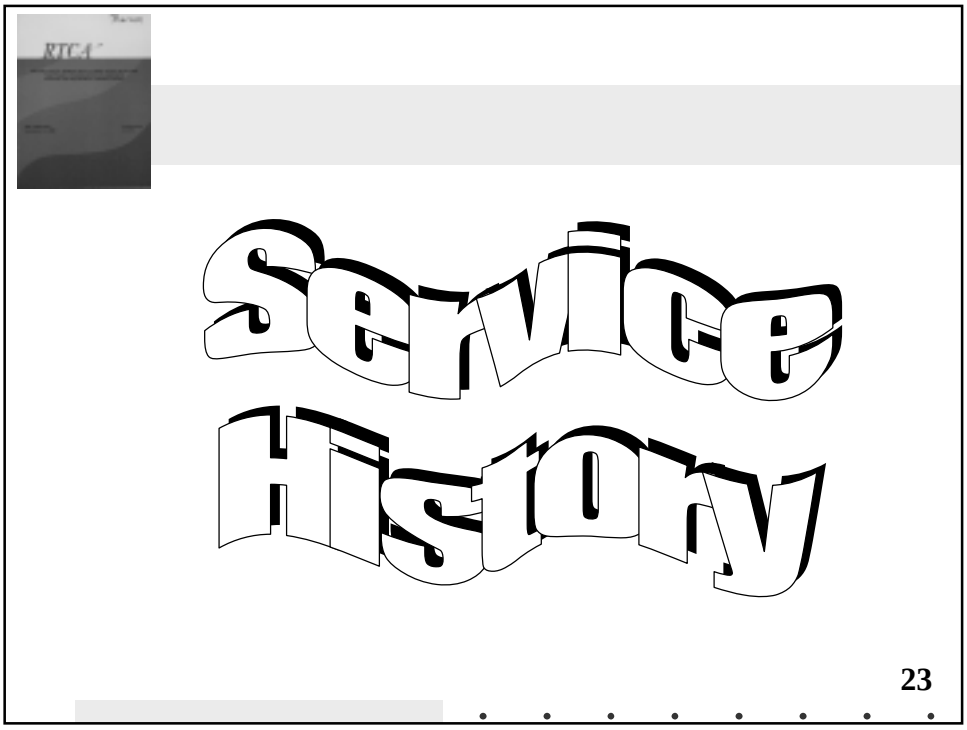
- FAQ #35 – Testing low-level requirements
- FAQ #38 – Differences between integration “process” and “testing”
- FAQ #73 – Timing measurements during testing
- DP #15 – Relationship between regression testing and hardware changes

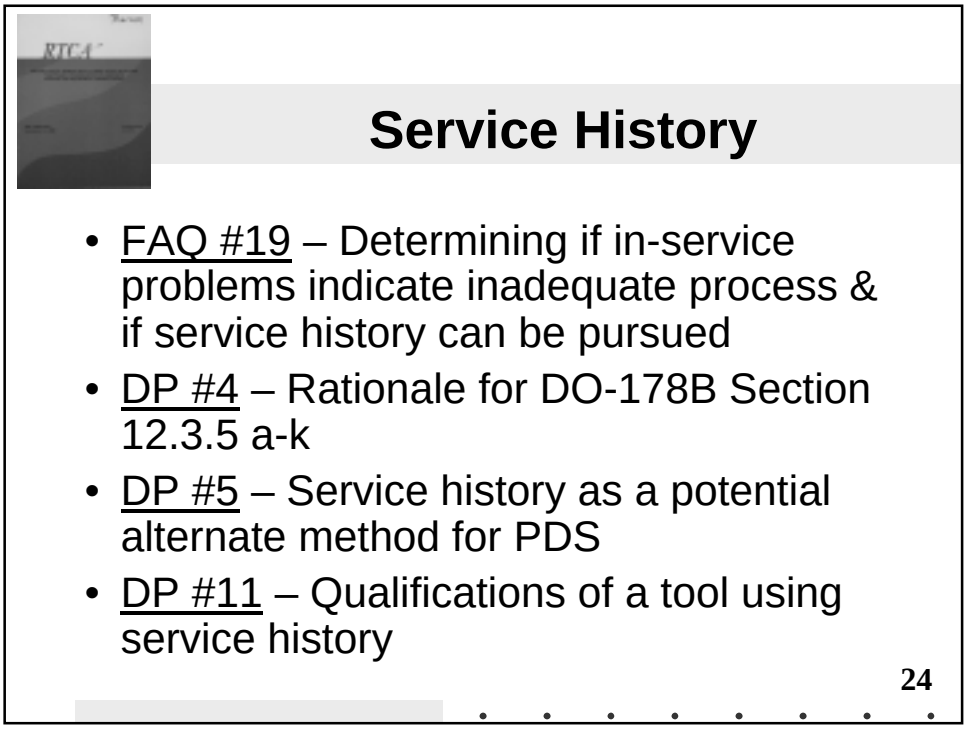
21

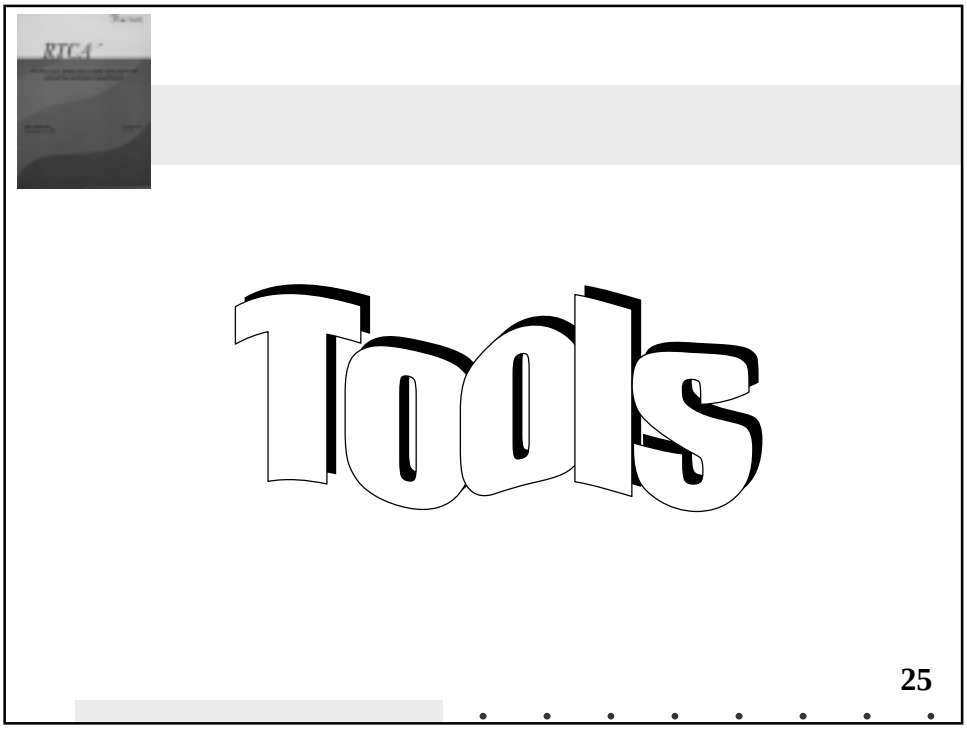
Verification – Data/Control Coupling

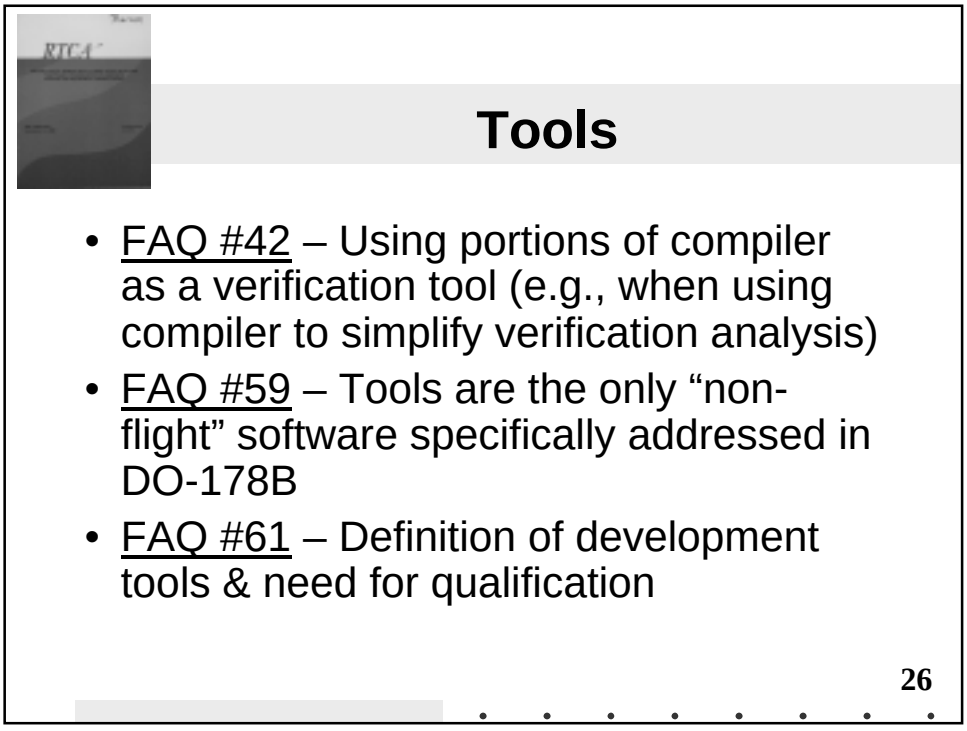
- FAQ #67 – Definition & verification of data/control coupling

22


Service
History
23


Service History
• FAQ #19 – Determining if in-service problems indicate inadequate process & if service history can be pursued
• DP #4 – Rationale for DO-178B Section 12.3.5 a-k
• DP #5 – Service history as a potential alternate method for PDS
• DP #11 – Qualifications of a tool using service history
24


Tools
25


Tools
• FAQ #42 – Using portions of compiler as a verification tool (e.g., when using compiler to simplify verification analysis)
• FAQ #59 – Tools are the only “non-flight” software specifically addressed in DO-178B
• FAQ #61 – Definition of development tools & need for qualification
26

Tools (cont)

- DP #1 – Verification tool selection considerations
- DP #11 – Qualification of a tool using service history

27

Control Categories

28

Control Categories

- FAQ #12 – Definition of CC1 & CC2
- FAQ #13 – Understanding Table 7-1 and CC1/CC2
- FAQ #14 – CC1/CC2 relationship to Annex A Tables
- FAQ #55 – Control category considerations when determining best approach to packaging of data

29

Other Interesting Topics

- Dead/Deactivated Code
  - FAQs #8, 28, 45, 70
- Traceability
  - FAQs #46 & 71; DP # 12
- Derived Requirements
  - FAQs #35, 36, 37
- Transition Criteria
  - DP #6

30

Other Interesting Topics (cont)

- Independence
  - FAQs #34, 36, & 74
- Integration
  - FAQs #28, 38, & 70
- Partitioning
  - DP #14
- Defensive Programming
  - FAQ #32

31

Other Interesting Topics (cont)

- Regression Analysis
  - DP #15
- Documentation
  - FAQs #51, 53, 54, 60

32

Summary

- DO-248B is planned for publication in September 2001
- DO-248B clarifies DO-178B
- DO-248B is not a guidance document
- Some of the major topics of DO-248B are PDS/COTS, verification, service history, tools, & control categories

33